Critical Infrastructure Security

Lecture 1

Dr. Naveed Anwar Bhatti

Webpage: naveedanwarbhatti.github.io

Who am I? Dr. Naveed Anwar Bhatti

Hometown: Islamabad

Last Job:
Senior Researcher
RISE, Stockholm, Sweden
Joined on April, 2018
ERCIM Post-Doc (April, 2018 – Sep, 2019)

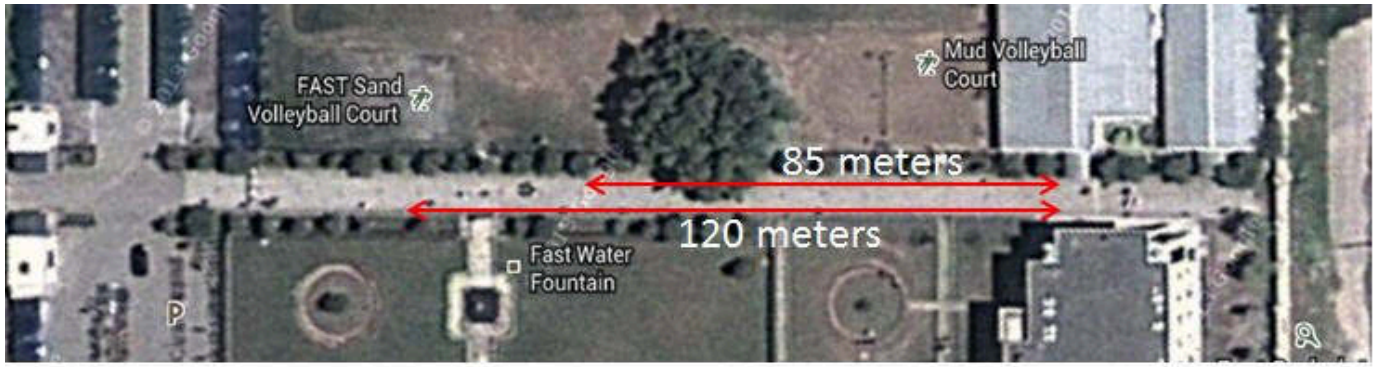
Education:

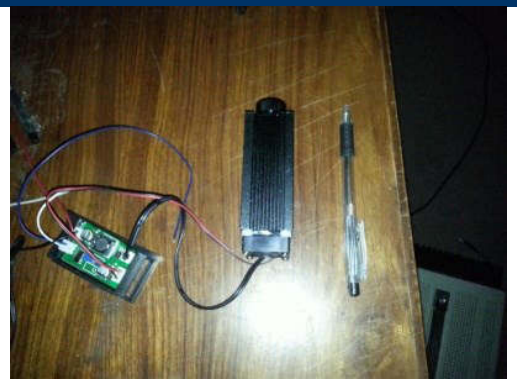
PhD 2018
Computer Science
Politecnico di Milano, Italy
System Support for Transiently Powered Embedded Systems

MS 2013
Computer Science
FAST-NUCES, Islamabad, Pakistan
Long range RFID System: Decoupling sensing and energy in sensor networks using energy transferenc

BS 2011
Telecom
FAST-NUCES, Islamabad, Pakistan
Internet Controlled Unmanned Ground Vehicle

Long range RFID-like System

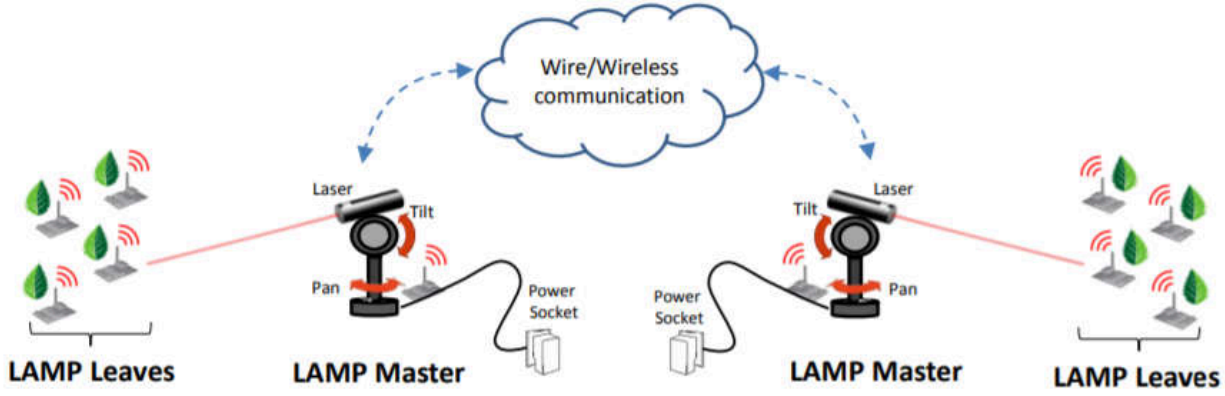




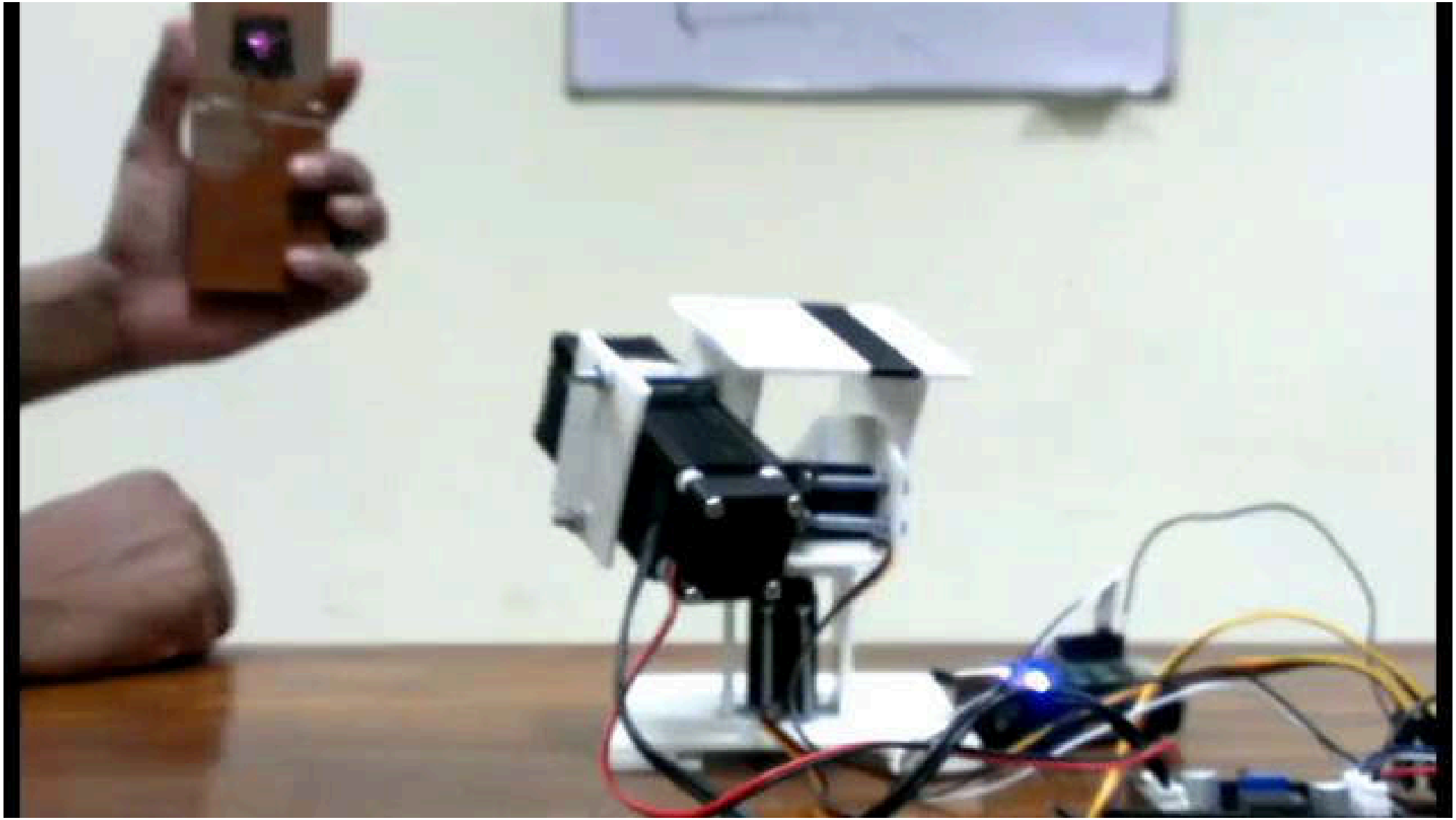
Laser Module

TelosB mote

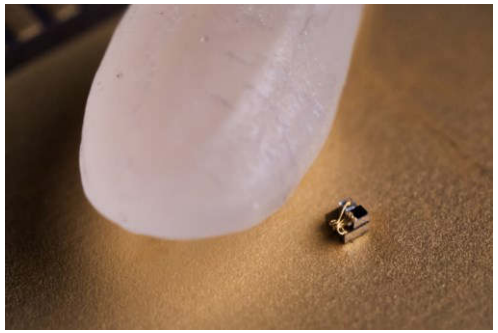
Solar Panel

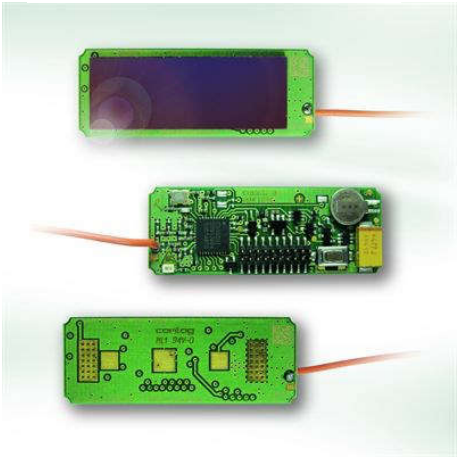


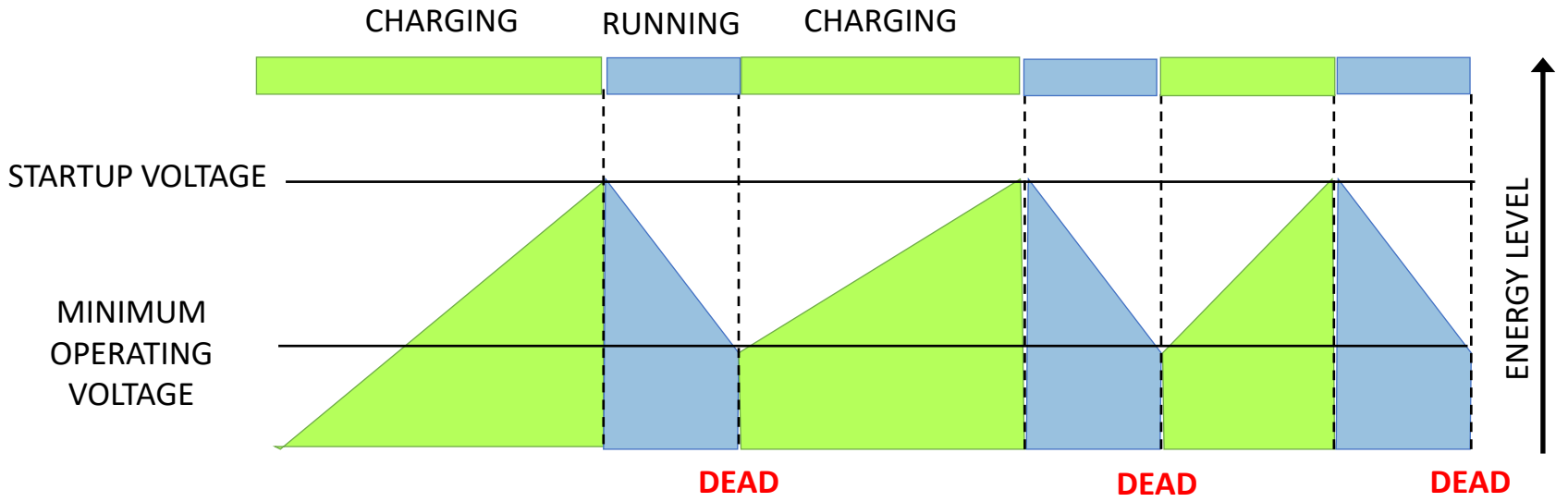
Long range RFID-like System

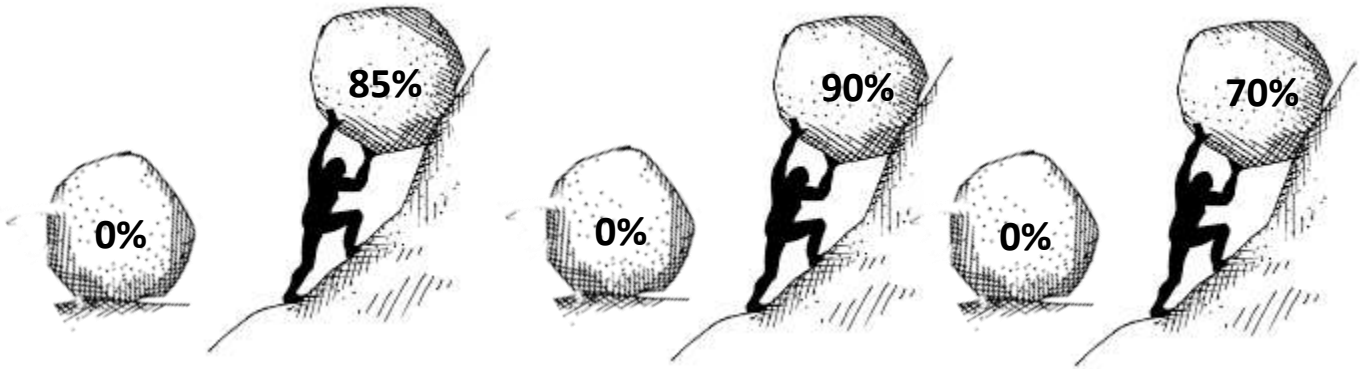


System Support for Transiently Powered Embedded Systems



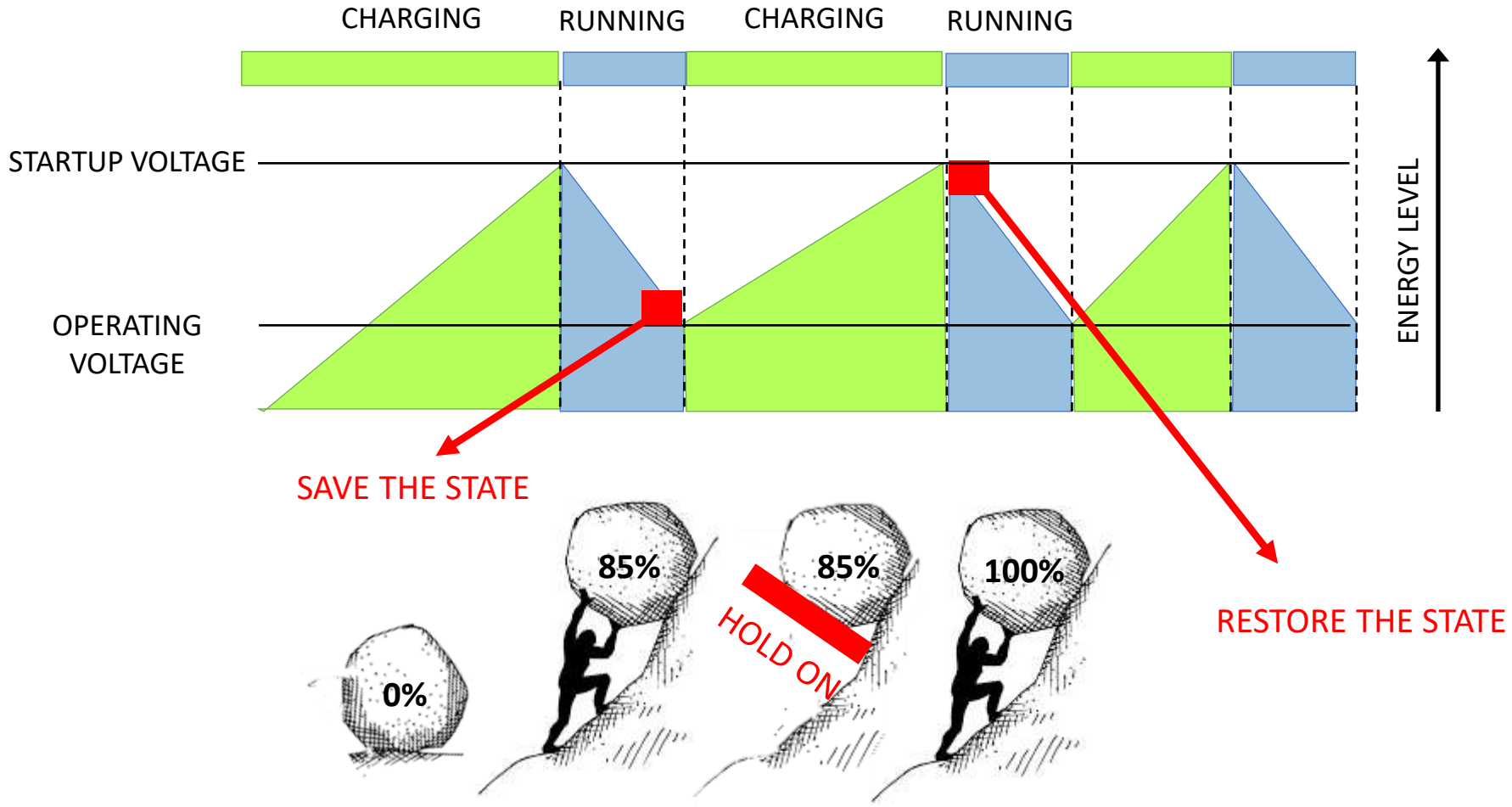




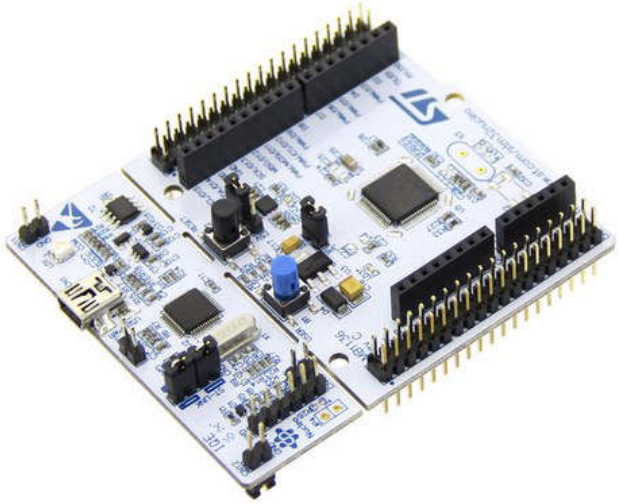


CHALLENGE: MAKE EMBEDDED DEVICES IMMUNE TO TRANSIENT POWER ENVIRONMENT

System Support for Transiently Powered Embedded Systems

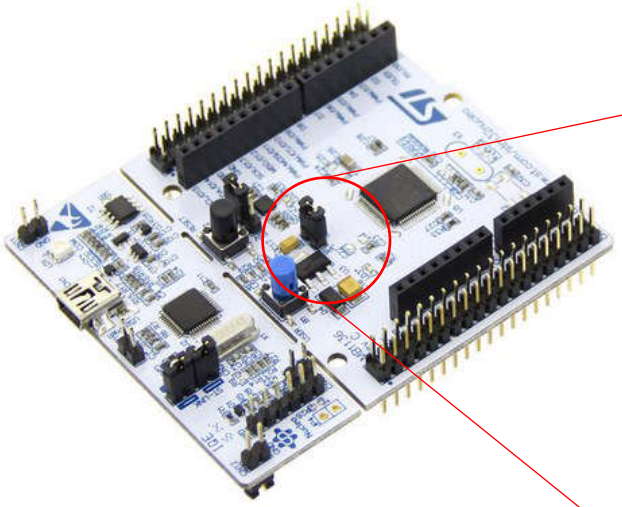


System Support for Transiently Powered Embedded Systems



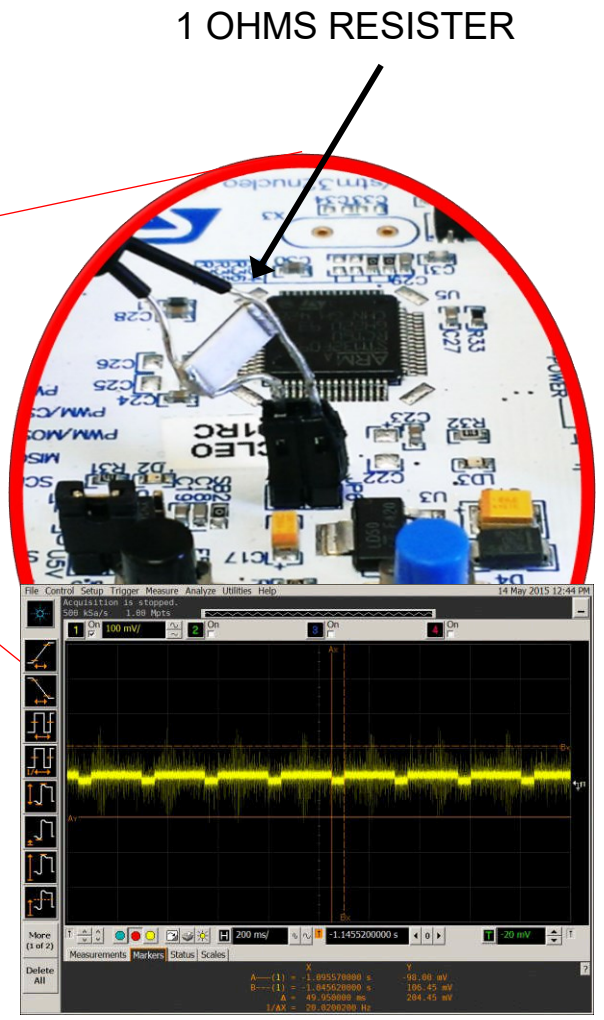
STM32 NUCLEO L152RE

ARM®32-bit Cortex®-M3 CPU
32 MHz max CPU frequency
512 KB Flash
80 KB SRAM

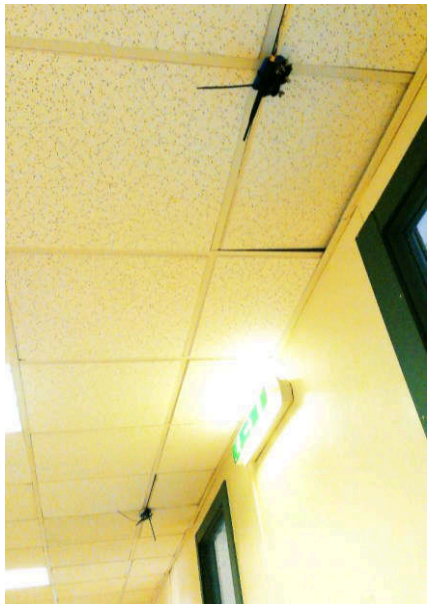


STM32 NUCLEO 91RC

ARM®32-bit Cortex®-M0 CPU
48 MHz max CPU frequency
256 KB Flash
32 KB SRAM

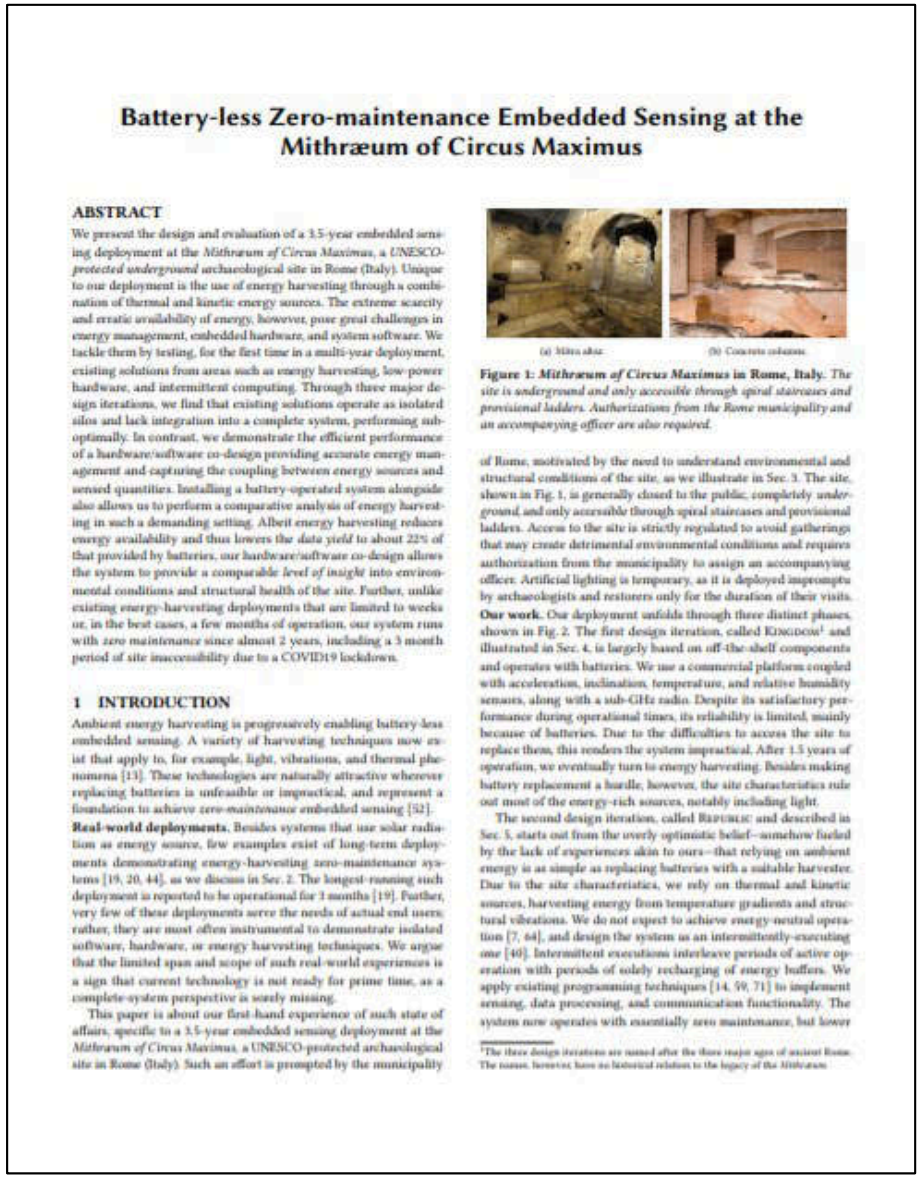


Other Sensor Deployments



Waspmote

Other Sensor Deployments



Battery-less Zero-maintenance Embedded Sensing at the Mithræum of Circus Maximus

ABSTRACT

We present the design and evaluation of a 3.5-year embedded sensing deployment at the *Mithræum of Circus Maximus*, a *UNESCO-protected underground* archaeological site in Rome (Italy). Unique to our deployment is the use of energy harvesting through a combination of thermal and kinetic energy sources. The extreme scarcity and erratic availability of energy, however, pose great challenges in energy management, embedded hardware, and system software. We tackle them by testing, for the first time in a multi-year deployment, existing solutions from areas such as energy harvesting, low-power hardware, and intermittent computing. Through three major design iterations, we find that existing solutions operate as isolated silos and lack integration into a complete system, performing sub-optimally. In contrast, we demonstrate the efficient performance of a hardware/software co-design providing accurate energy management and capturing the coupling between energy sources and sensed quantities. Installing a battery-operated system alongside also allows us to perform a comparative analysis of energy harvesting in such a demanding setting. Albeit energy harvesting reduces energy availability and thus lowers the *data yield* to about 22% of that provided by batteries, our hardware/software co-design allows the system to provide a comparable *level of insight* into environmental conditions and structural health of the site. Further, unlike existing energy-harvesting deployments that are limited to weeks or, in the best cases, a few months of operation, our system runs with *zero maintenance* since almost 2 years, including a 3 month period of site inaccessibility due to a COVID19 lockdown.

1 INTRODUCTION

Ambient energy harvesting is progressively enabling battery-less embedded sensing. A variety of harvesting techniques now exist that apply to, for example, light, vibrations, and thermal phenomena [13]. These technologies are naturally attractive wherever replacing batteries is unfeasible or impractical, and represent a foundation to achieve *zero-maintenance* embedded sensing [52].

Real-world deployments. Besides systems that use solar radiation as energy source, few examples exist of long-term deployments demonstrating energy-harvesting zero-maintenance systems [19, 20, 44], as we discuss in Sec. 2. The longest-running such deployment is reported to be operational for 3 months [19]. Further, very few of these deployments serve the needs of actual end users; rather, they are most often instrumental to demonstrate isolated software, hardware, or energy harvesting techniques. We argue that the limited span and scope of such real-world experiences is a sign that current technology is not ready for prime time, as a complete-system perspective is sorely missing.

This paper is about our first-hand experience of such state of affairs, specific to a 3.5-year embedded sensing deployment at the *Mithræum of Circus Maximus*, a UNESCO-protected archaeological site in Rome (Italy). Such an effort is prompted by the municipality

(a) Mithræum altar. (b) Concrete columns.

Figure 1: *Mithræum of Circus Maximus* in Rome, Italy. *The site is underground and only accessible through spiral staircases and provisional ladders. Authorizations from the Rome municipality and an accompanying officer are also required.*

of Rome, motivated by the need to understand environmental and structural conditions of the site, as we illustrate in Sec. 3. The site, shown in Fig. 1, is generally closed to the public, completely underground, and only accessible through spiral staircases and provisional ladders. Access to the site is strictly regulated to avoid gatherings that may create detrimental environmental conditions and requires authorization from the municipality to assign an accompanying officer. Artificial lighting is temporary, as it is deployed impromptu by archaeologists and restorers only for the duration of their visits.

Our work. Our deployment unfolds through three distinct phases, shown in Fig. 2. The first design iteration, called KINGDOM[1] and illustrated in Sec. 4, is largely based on off-the-shelf components and operates with batteries. We use a commercial platform coupled with acceleration, inclination, temperature, and relative humidity sensors, along with a sub-GHz radio. Despite its satisfactory performance during operational times, its reliability is limited, mainly because of batteries. Due to the difficulties to access the site to replace them, this renders the system impractical. After 1.5 years of operation, we eventually turn to energy harvesting. Besides making battery replacement a hurdle, however, the site characteristics rule out most of the energy-rich sources, notably including light.

The second design iteration, called REPUBLIC and described in Sec. 5, starts out from the overly optimistic belief—somehow fueled by the lack of experiences akin to ours—that relying on ambient energy is as simple as replacing batteries with a suitable harvester. Due to the site characteristics, we rely on thermal and kinetic sources, harvesting energy from temperature gradients and structural vibrations. We do not expect to achieve energy-neutral operation [7, 64], and design the system as an intermittently-executing *one* [40]. Intermittent executions interleave periods of active operation with periods of solely recharging of energy buffers. We apply existing programming techniques [14, 59, 71] to implement sensing, data processing, and communication functionality. The system now operates with essentially zero maintenance, but lower

[1]The three design iterations are named after the three major ages of ancient Rome. The names, however, have no historical relation to the legacy of the Mithræum.

“Battery-less Zero-maintenance Embedded Sensing at the Mithraeum of Circus Maximus”

SenSys 2020

How to reach me?

Email: naveed.bhatti@mail.au.edu.pk
Webpage: naveedanwarbhatti.github.io

Class page and slides: **7xuqefo** (Google classroom)

Course Outline: Why are you here?

- Critical Infrastructures

Week 1, 2

- Objectives and outline
- Intro to Critical Infrastructure
- Critical Infrastructure and Cyber Physical Systems
- Cyber Security
- Why do we need to secure Critical Infrastructure?
- Components of CPS
- Cyber world & physical world
- Information Technology & Operation Technology
- Ways of modeling CPS

- Cyber Security Concepts

Week 3, 4, 5

- Vulnerabilities
- Threats & Threat actors
- Attacks & Attack vectors
- Risk
- Types of security
- Intrusion detection
- Incident response
- Forensics
- Risk management
- Security governance
- Training & awareness

Course Outline: Why are you here?

- Threats and Countermeasures for CIS

  Week 6 and 7

  - Organizational threats
  - Architecture threats
  - Communication threats
  - Operational threats
  - Risk Management in Critical Infrastructure
  - Intrusion Detection in Critical Infrastructure
  - Incident Response in Critical Infrastructure

- Case Studies

  Week 8

  - Stuxnet
  - IoT
  - Smart Vehicle
  - Embedded System

- Paper Presentations

  Week 9, 10, 11, 12

Administrivia and more

- **Grading split**
  - Assignments: 20%
  - ~~Quizzes: 0%~~
  - Mid-Term Exam: 25%
  - Project (Research Paper): 10%
  - Final Exam: 45%

Will be presentation

- Allow for in-depth study of things discussed in class

Presentations

- Cybersecurity of Smart Electric Vehicle Charging: A Power Grid Perspective
- Who's in Control of Your Control System? Device Fingerprinting for Cyber-Physical Systems.
- Hey, My Malware Knows Physics! Attacking PLCs with Physical Model Aware Rootkit.
- Cyber-security on smart grid: Threats and potential solutions
- RFDIDS: Radio Frequency-based Distributed Intrusion Detection System for the Power Grid
- Lest We Remember: Cold Boot Attacks on Encryption Keys
- Light commands: laser-based audio injection attacks on voice-controllable systems
- What You Corrupt Is Not What You Crash: Challenges in Fuzzing Embedded Devices
- Toward the Analysis of Embedded Firmware through Automated Re-hosting
- Adversarial Attacks against LiDAR Semantic Segmentation in Autonomous Driving

Structure of Presentation (Like TPC)

Presenter

Defender

Opponent

The presenter gives a neutral presentation. (~ 20 minutes)

The defender and the opponent present their arguments for and against the paper. (At most 5 minutes each)

- We have a regular discussion about the paper (5 to 10min).
- We vote on whether the paper should be accepted or rejected, imagining that we are the **technical program committee** (**TPC**) for a conference of equivalent standard as the one where the paper was published.

Structure of Presentation (Like TPC)

- Each student must select:.
  - **2 papers for presentation**
  - **2 papers as a defender**
  - **2 papers as a opponent**

Note:
- Please select your papers by **16th Feb 2022**.
- Google Excel Sheet Uploaded on GCR

- We will have one presentation every **Wednesday**

- All students (**except presenter**) will submit **reviews** on weekly basis before the presentation (**deadline Wednesday 11:59pm**) of the paper that will presented that week

Structure of Presentation (Like TPC)

- **Structure of a Review:**
  - Summary
  - Strength -> in bullet points
  - Weakness -> in bullet points
  - Detail Comments
  - Recommendation
    - **Strong Accept**
    - **Accept**
    - **Reject**
    - **Strong Reject**

Review #9C [Hae Young Noh] R1 24 Nov 2018

Overall merit
3. Weak accept

Reviewer expertise
2. Some familiarity

Paper summary
This paper introduces a TED algorithm to decode signals from satellites for Space IoT applications. The signals are often very noisy and Doppler influenced, which makes it difficult to decode, and the authors use a combination of filters and Teager Energy Operator to effectively extract information. The algorithm is evaluated with data received from two nanosatellites, and its performance is compared with other COTS transceivers.

Strengths
+ Space IoT is a new and interesting topic
+ The algorithm is evaluated with signals from two satellites. It performed consistently better than the two COTS transceivers.
+ The algorithm is shown to be particularly robust to low SNR

Weaknesses
– The overall method seems to be a combination of existing methods.
– Low energy consumption and complexity are claimed as a contribution but not evaluated.

Comments for author
This paper presents an interesting and timely topic of Space IoT. The authors propose a new algorithm to communicate between satellites and low-power sensor nodes. The paper clearly explains the challenges associated with decoding the satellite signals, such as Doppler shifts and high level of noise. The paper provides thorough explanations and examples of satellite signals and how to address these challenges. However, there are several concerns about the paper:

1) The authors claim that they have advanced the state of the art in decoding, but the proposed method mostly seems to be a combination of existing methods such as bandpass filtering, matched filter, and TEO. Overcoming Doppler shifts has been extensively studied before in multiple fields. What additional challenge does the "context of space IoT" introduce? Without this clarification, their claim about this research contribution is not convincing.

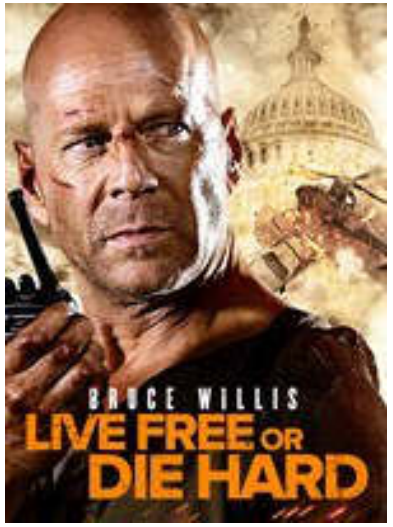
2) There are 8 research contributions discussed in the Introduction. However, many of them seem to be repetitive and can be merged. For example, contributions 2, 4, 5, and 6 may be combined and 7

Prerequisites and Expectations

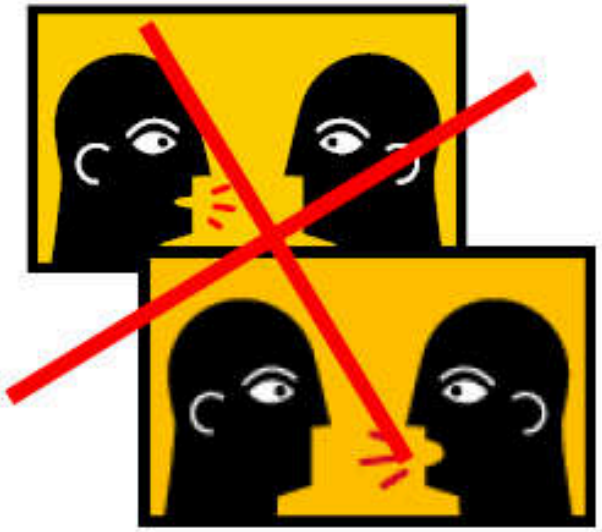
- **Everyone should already:**
  - Have basic electronics knowledge
  - Know how to read and dissect paper (quickly)

- **Need to be willing to learn and take initiative (very little spoon feeding)**

- **Movies:**
  - Die-hard 4
  - Angel Has Fallen
  - Geostorm



Prohibitions



Class Attendance and Late arrival

- **University and HEC cares about it**
  - **I do not !**
  - I shall say you are present as long as you tell me before class
  - If you are not serious about the course, its your loss
    - Both money wise
    - And grade wise (directly: 10% participation, quizes indirectly: exams)

- **If you arrive late**
  - Be discrete (come in with minimal fanfare)
  - Be courteous (to other students trying to listen)

What's Wrong With This Picture?

What's Wrong With This Picture?

Critical Infrastructures

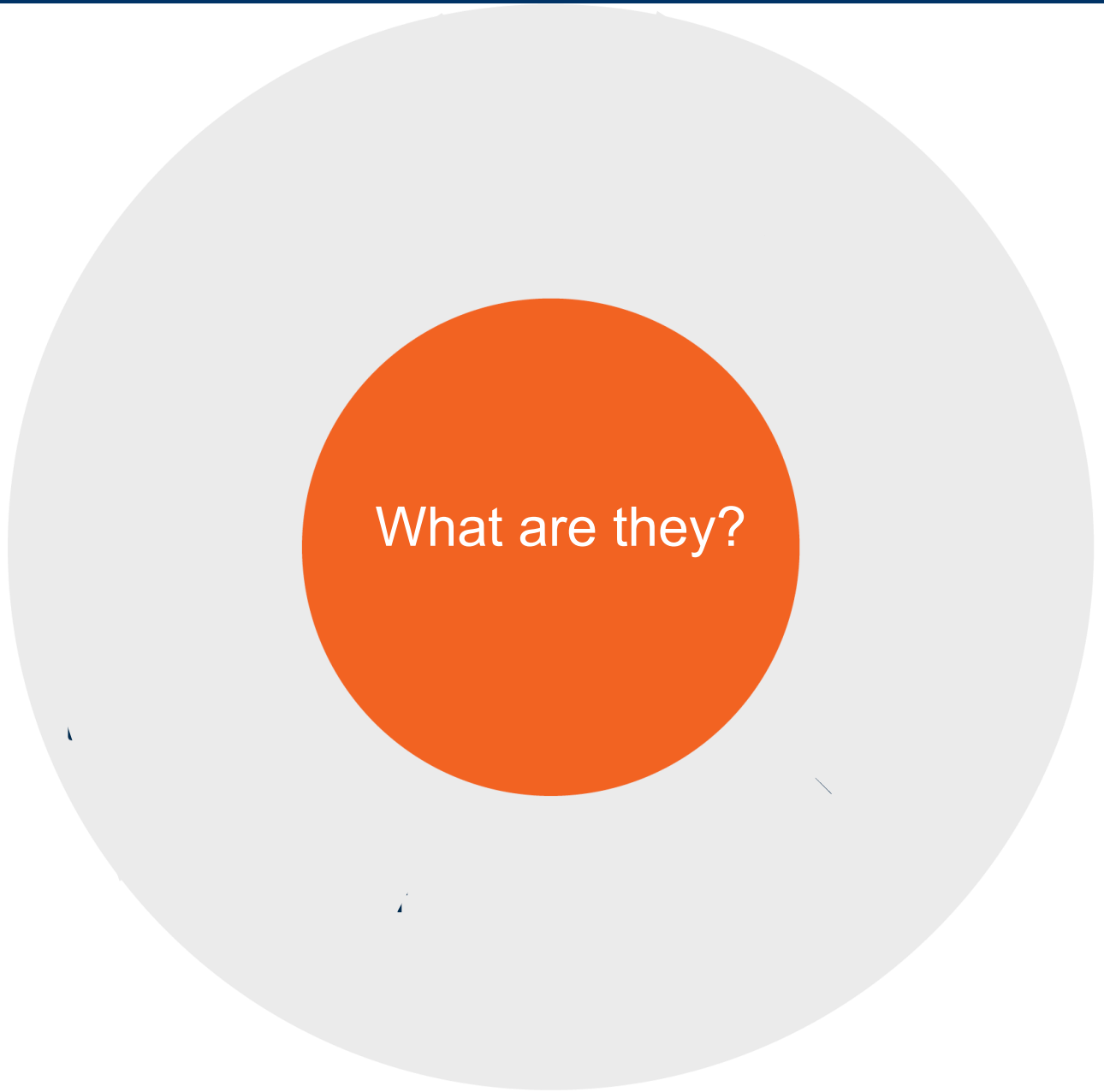
- What are they?
- Why do we care?

Definitions of “ Critical Infrastructure”

- Critical infrastructure refers to **processes**, **systems**, **facilities**, **technologies**, **networks**, **assets** and **services** essential to the **health**, **safety**, **security** or **economic well-being** of citizens and the effective functioning of government.

- Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders.

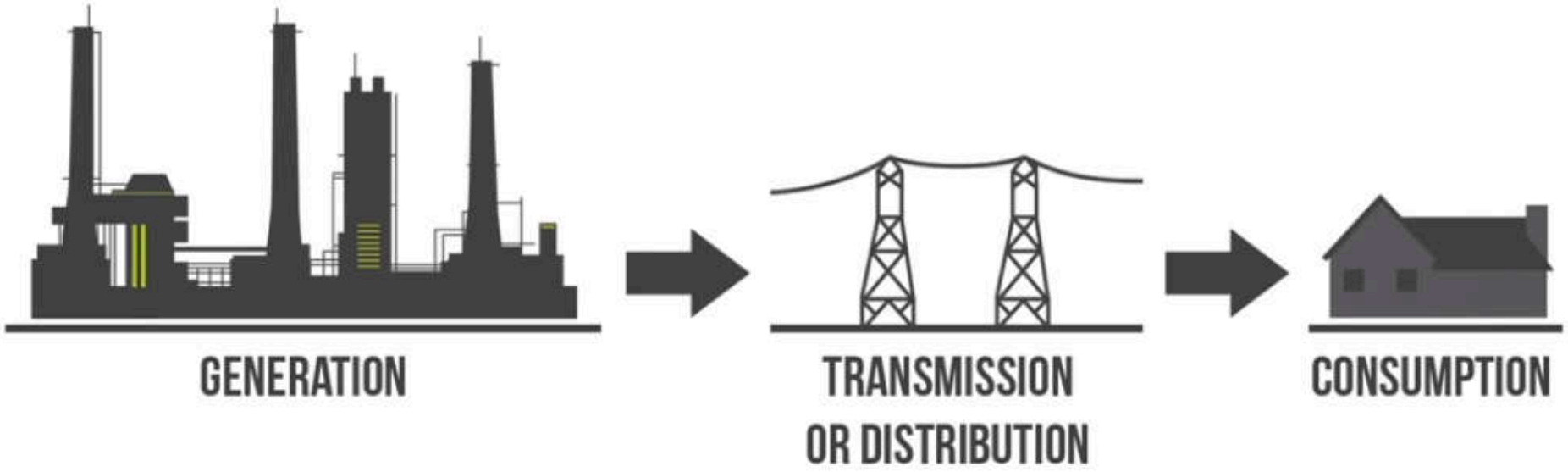
Critical Infrastructure



Electricity Grid (Electric Grid, Electrical Grid or Power Grid)

- The electrical grid is the electrical power system network comprised of:
  - Generating plant
  - Transmission lines
  - Substation
  - Transformers
  - Distribution lines
  - Consumer.

- The electrical grid is divided into three main components

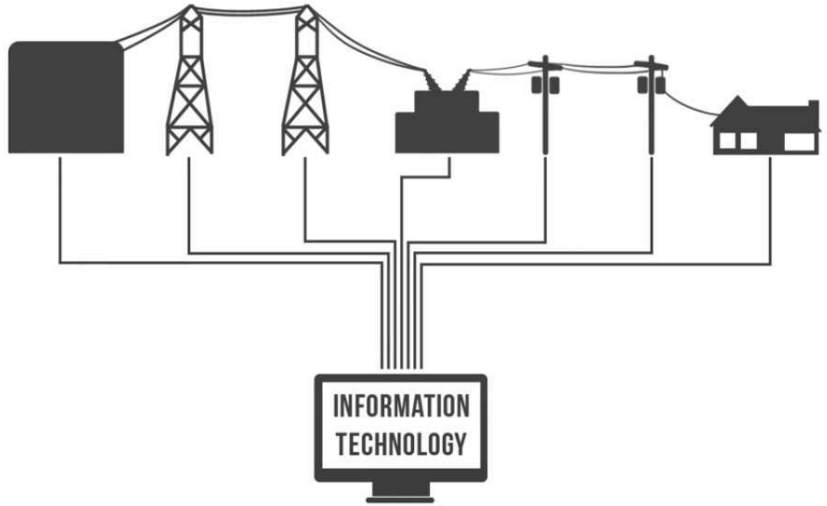


Electricity Grid

- Electric power distribution systems historically have incorporated little automation

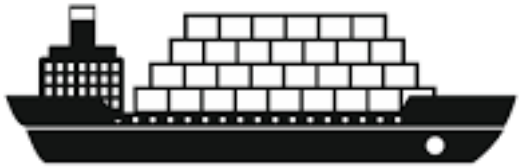
- In response **to growing demands** to improve reliability, automation is being implemented in power distribution systems

- Key element in enabling automation and smart grid applications ***Information Technology***.
  - Automated Substation Reconfiguration
  - Automated Load Balancing
  - Automatically Read Utility Meters
  - Automated FCI (fault circuit indicator) Monitoring
  - Much more…

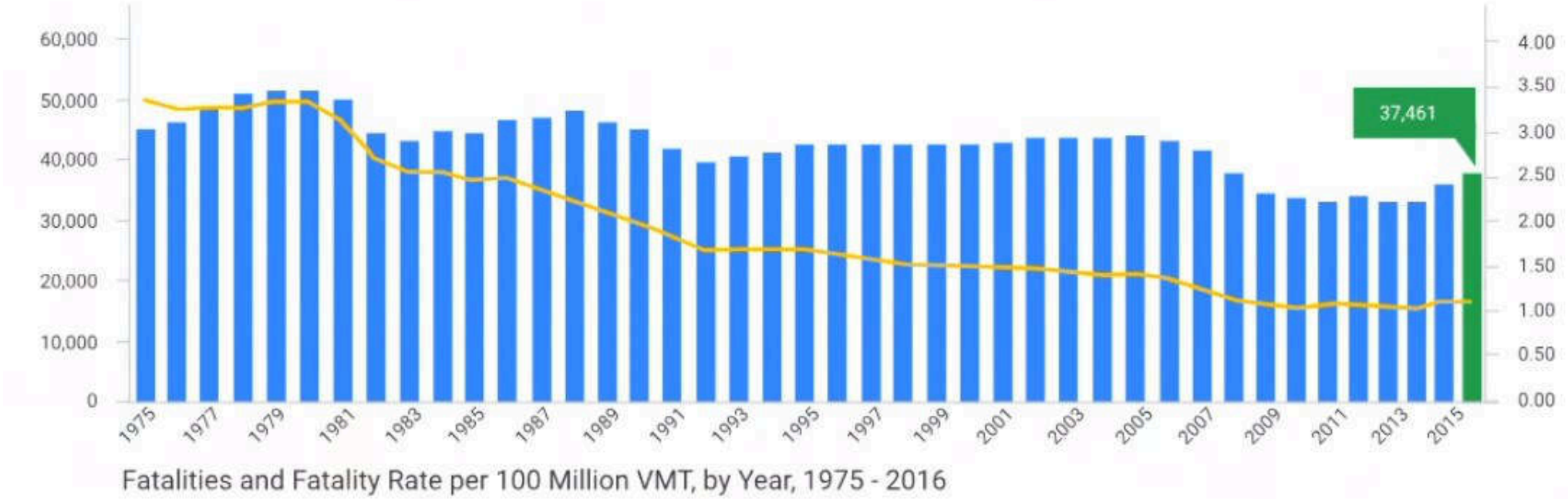


Transportation System

- Allows citizens to move from Point A to Point B
- Different modes of transportation:
  - **Airports:** Transport people and goods long distances in a short period of time
  - **Passenger and freight rail lines:** Transport people and goods regionally/nationally
  - **Subway lines or light rail corridors (in large urban centers):** Transport people to/from work and entertainment/leisure activities
  - **Harbors and ports:** Import/export goods from/to the globally and distribute them on inland
  - **Ferry terminals and waterways:** Transport the workforce to/from work (e.g., San Francisco, New



Transportation System



Fatalities and Fatality Rate per 100 Million VMT, by Year, 1975 - 2016

Roads, Railways and Waters are busier, heavily **congested …**

Average commuter in big urban city experience 3 hours of delay everyday

… and **dangerous**

Trends show that by 2030, road injuries will become the seventh leading cause of death

Intelligent Transportation System

- Application of ***Information Technology*** for Transportation solution
  - Traffic Management Centers (TMC)
  - Devices/Infrastructure
    - CCTV, Radar, Sensors
  - Communication
    - Realtime VMS (variable message sign)
    - Vehicle-to-Vehicle (V2V)
    - Adoptive Traffic Signal

- Improves Traveler:
  - Safety
  - Convenience
  - Efficiency

- High return on investment

Why do we care?

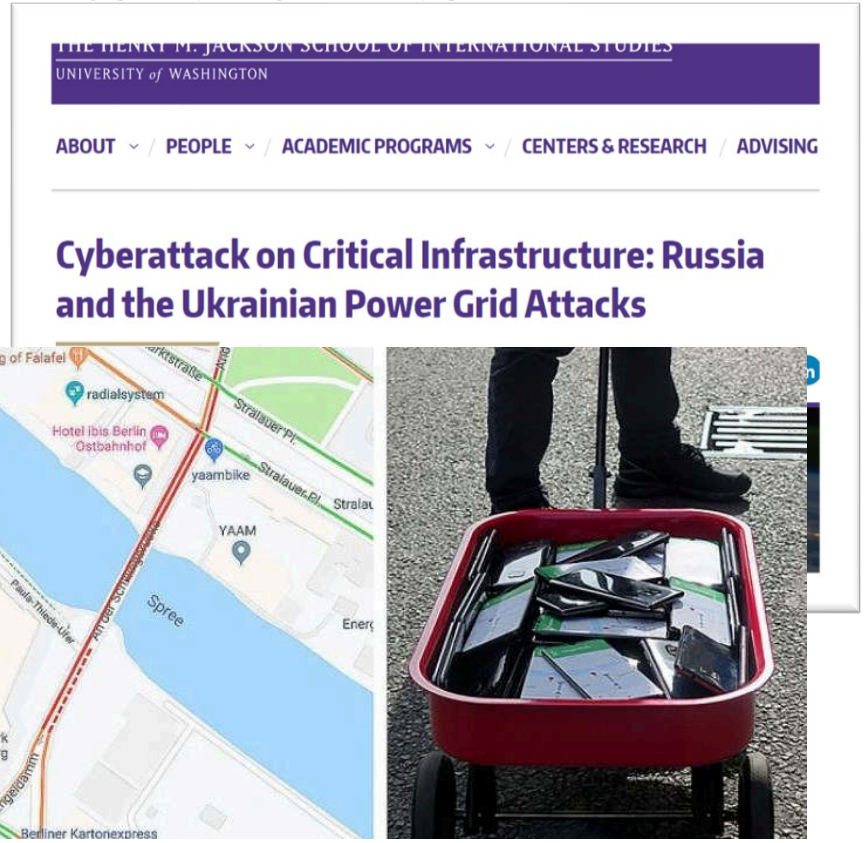
- Disruptions of critical infrastructure could **result in catastrophic** loss of **life**, **adverse economic effects** and **significant harm to public confidence**.

Power grid disturbances

Ukraine power grid incident - Malware attacked several substations, leaving hundreds of thousands of homes without electricity

Traffic control problems

In The Netherlands, researchers demonstrated that they could control traffic lights of 10 cities through Internet!



What makes attack possible?

- Critical infrastructures are key targets for cyberattacks because of their extensive use of **cyber-physical systems.**

- **“Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other.” - NSF**

Cyber-Physical Systems (CPS)

- Some terms that we have already heard are all CPS!
  - **IoT**
  - **WSN**
  - **ICS**
  - **SCADA**
  - **Smart phones**
  - **Smart vehicles**
  - **Smart cities**
  - **And the list goes on…**

Cyber-Physical Systems (CPS)

- Two broad categories
  - Infrastructural
    - Focus on physical dimension
    - Cyber dimension is added for enhancing efficiency and productivity
    - Examples: Smart - power grid, transportation, industry
  - Personal
    - Focuses on cyber dimension
    - Physical dimension is added to enhance the utility of the information system
    - Examples: Smart - phone, smart watches, wearables

Cyber Security

- "**Cybersecurity** is the convergence of people, processes and technology that come together to protect organizations, individuals or networks from **digital attacks**" – CISCO

- What kind of attacks? The attacks on the **CIA** triad:
  - Confidentiality
    - Data/system is only visible/accessible to authorized person(s)
  - Integrity
    - Data/system is only modified/operated by authorized person(s)
  - Availability
    - Data/system is available for use by authorized person(s)

Cyber Security

- Where can an attack be launched on digital data?
  - Stored data
    - Hard disk, USB device, Cloud
  - Data being processed
    - Processor, RAM
  - Data being transmitted
    - Wired or wireless network, inter-device communication
  - Data being generated
    - Data acquisition, sensors

Secure Critical Infrastructure from whom?

- Novice hackers
- Malicious hackers
- Hacktivists
- Anti-state actors

How to secure Critical Infrasturcture?

- People
  - Designers
  - Managers
  - Users
- Processes
  - Asset management
  - Risk management
  - Policy making, revision and enforcement
  - Contingency planning
  - Training and awareness
- Technology
  - Tools for threat monitoring, detection and mitigation

CPS Background

- CPS originated from embedded systems
  - Embedded systems are characterized by their tight integration of hardware-software components and interaction with physical world
- What makes Cyber component of CPS different from IT?
  - Focus is more on availability
  - The actions performed by a CPS are often irreversible
- The cyber component of CPS is also called Operational Technology (OT)

CPS components

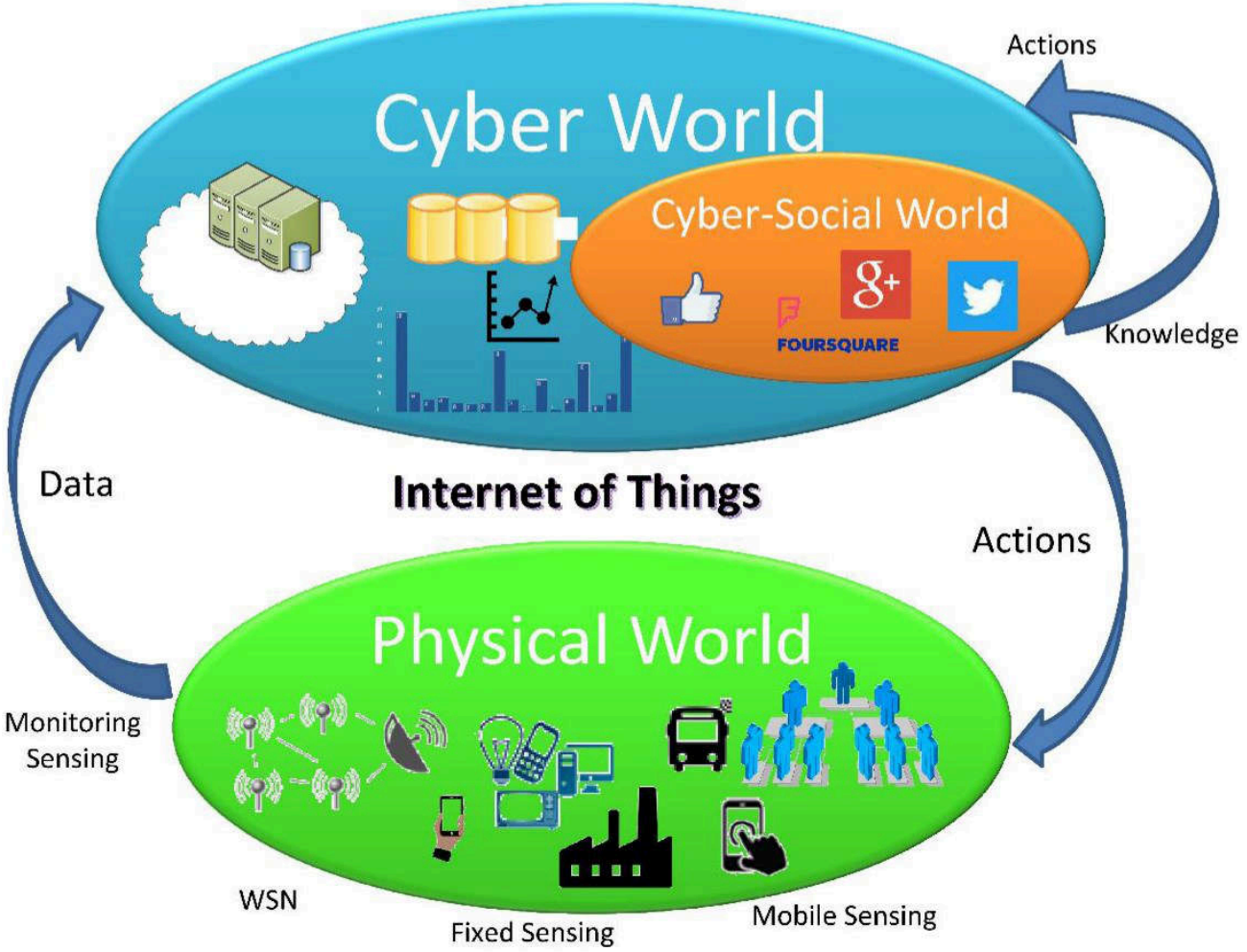
- Sensors
- Actuators
- Network
- Computer
- Physical process

- Are these individual components or we can somehow make a grouping?

Modeling CPS: Two-layer model

- Physical world and Cyber world
  - **Physical world**
    - Sensing (monitoring)
    - Actuating (controlling)
  - **Cyber world**
    - Communication
    - Computing

Modeling CPS: Two-layer model

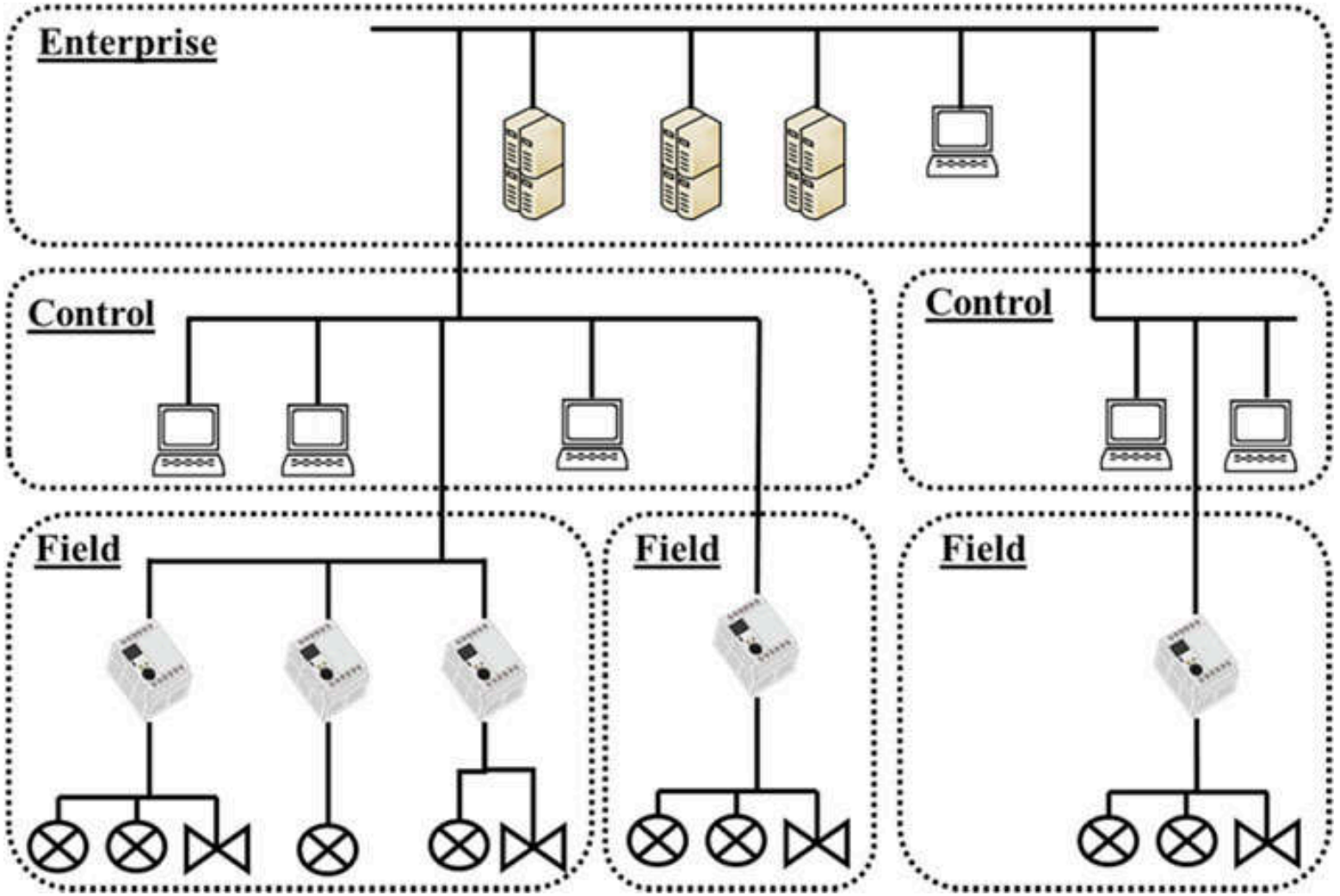


De, Suparna & Zhou, Yuchao & Abad, Iker & Moessner, Klaus. (2017). Cyber–Physical–Social Frameworks for Urban Big Data Systems: A Survey. Applied Sciences. 7. 1017. 10.3390/app7101017.

Modeling CPS – Three-tier model

- Enterprise zone
- Control zone
- Field zone

Modeling CPS – Three-tier model



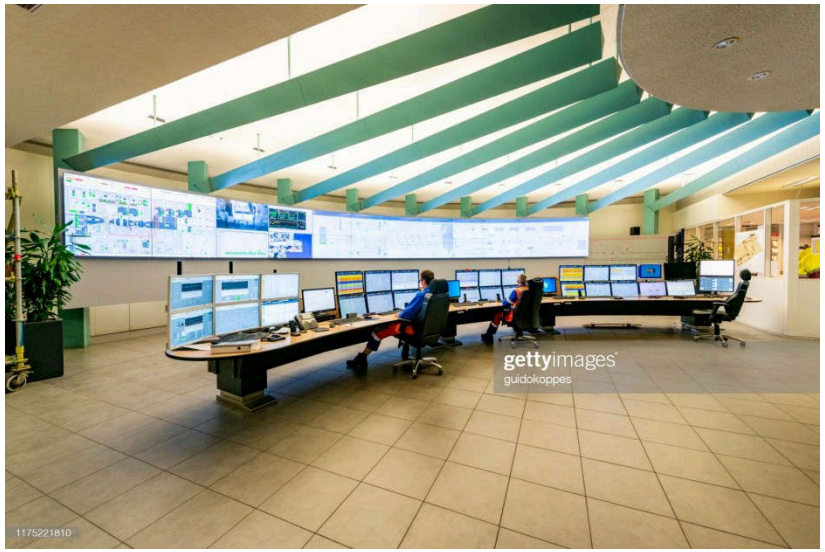
Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

Modeling CPS – Three-tier model

- Enterprise zone
  - Enterprise systems
  - Business networks
  - End-point devices that evolve rapidly and are updated frequently
  - Not connected with systems in operational zone in the usual manner
  - Cybersecurity solutions from general IT domain are applied to secure this zone

Modeling CPS – Three-tier model

- Control zone
  - The ‘control room’ environment
  - SCADA interfaces
  - Control elements for the processes
  - Contains systems and networks but these are kept separate from the enterprise zone
  - Never connected to outside world
  - Systems and devices are not updated very frequently
  - General cybersecurity solutions are usually not enough



Modeling CPS – Three-tier model

- Field zone
  - The process or operation environment
  - Sensing and automation end-points
  - Embedded control systems/PLCs
  - Control Elements are connected through robust industrial protocols with tight timing constraints
  - Usual IT solutions never apply here

https://www.theengineer.co.uk/steaming-ahead-with-energy-recovery/

Modeling CPS – Three-tier model

- Each zone has its own security requirements
- It is crucial to establish well-defined boundaries between zones
- Not always possible to completely isolate the zones, but extreme caution must be exercised for implementing inter-zone interfaces

CPS Characteristics

- **Heterogeneity**
  - A CPS may consist of sub-CPS, which may have different set of hardware/software components and, may follow different communication protocols
- **Interoperability**
  - The capability of system components to connect, communicate, and operate with each other
    - A critical factor for interoperability is standardization because components have to understand each others communication
- **Modularity**
  - CPS may have plug-and-play capability for extending the control to new devices

CPS Characteristics

- **Service-orientation**
  - The functionality implemented by one component is easily available to other components as a service
- **Decentralization**
  - Different zones of a CPS have autonomous decision power – distributed control
- **Computational capability**
  - Enough computation power is required for systems in all zones to process the data at required speeds
- **Integration**
  - This is the key and defining characteristic of CPS
- **Intelligence**
  - The computing power alone is not enough; the control must be able to intelligently analyze data and take decisions

Safety and reliability in Critical Infrastructure

- Safety and reliability are important requirements in critical infrastructure
- These requirements determine every aspect of critical infrastructure design, operation and maintenance
- Such systems need to be *dependable* – the end-user must never be affected by a fault occurring in any of the zones
- Approaches for making systems dependable
  - **Fault avoidance**
  - **Fault removal**
  - **Fault tolerance**

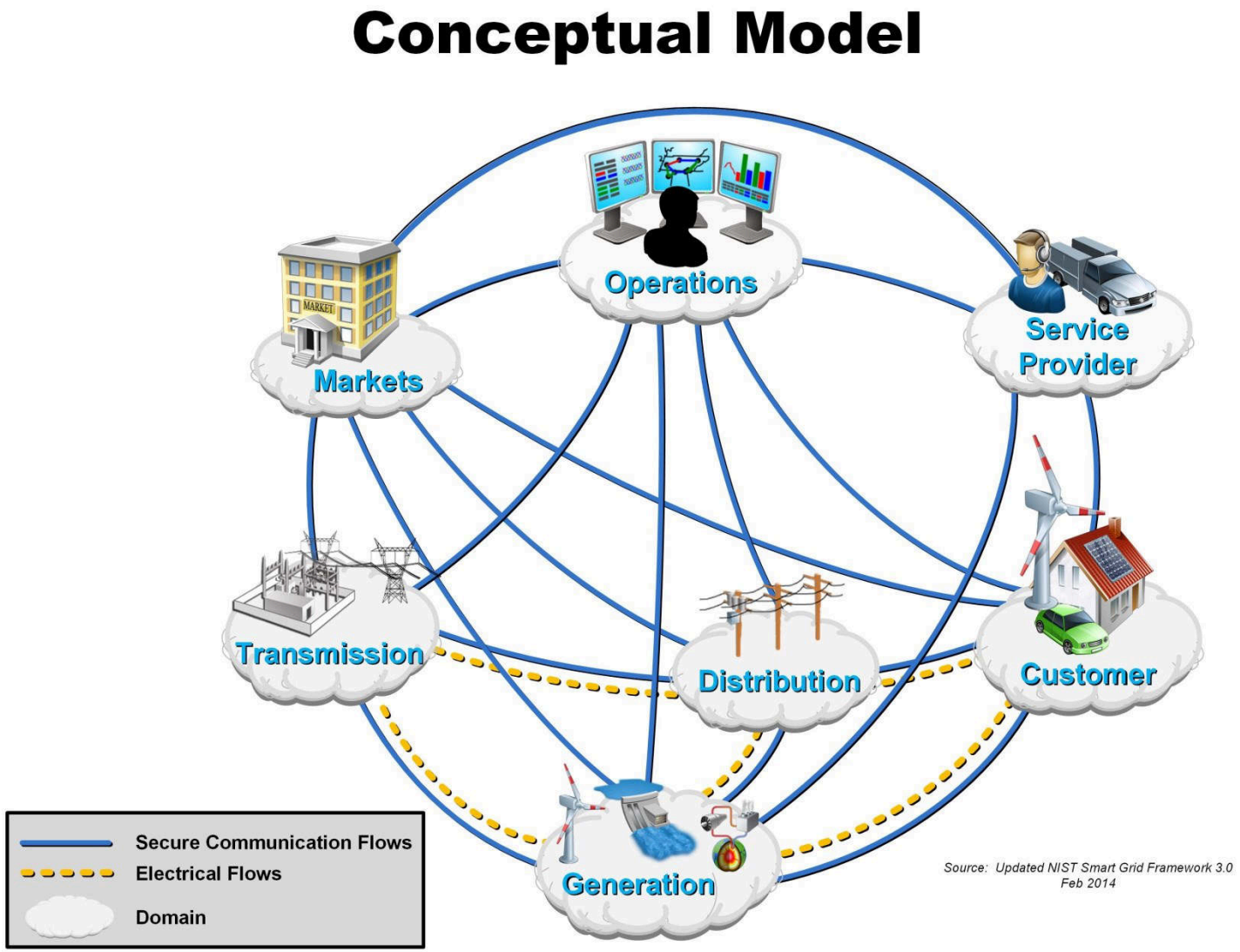
Fault tolerance

- Can be segregated into hardware and software fault tolerance
- Hardware fault tolerance achieved through **redundancy**
- Software fault tolerance requires
  - Diversity
  - Defense-in-depth
  - Monitoring
- The above techniques may effectively address random or design faults…
- But may not be enough to counter the effects of cyber attacks. Why?

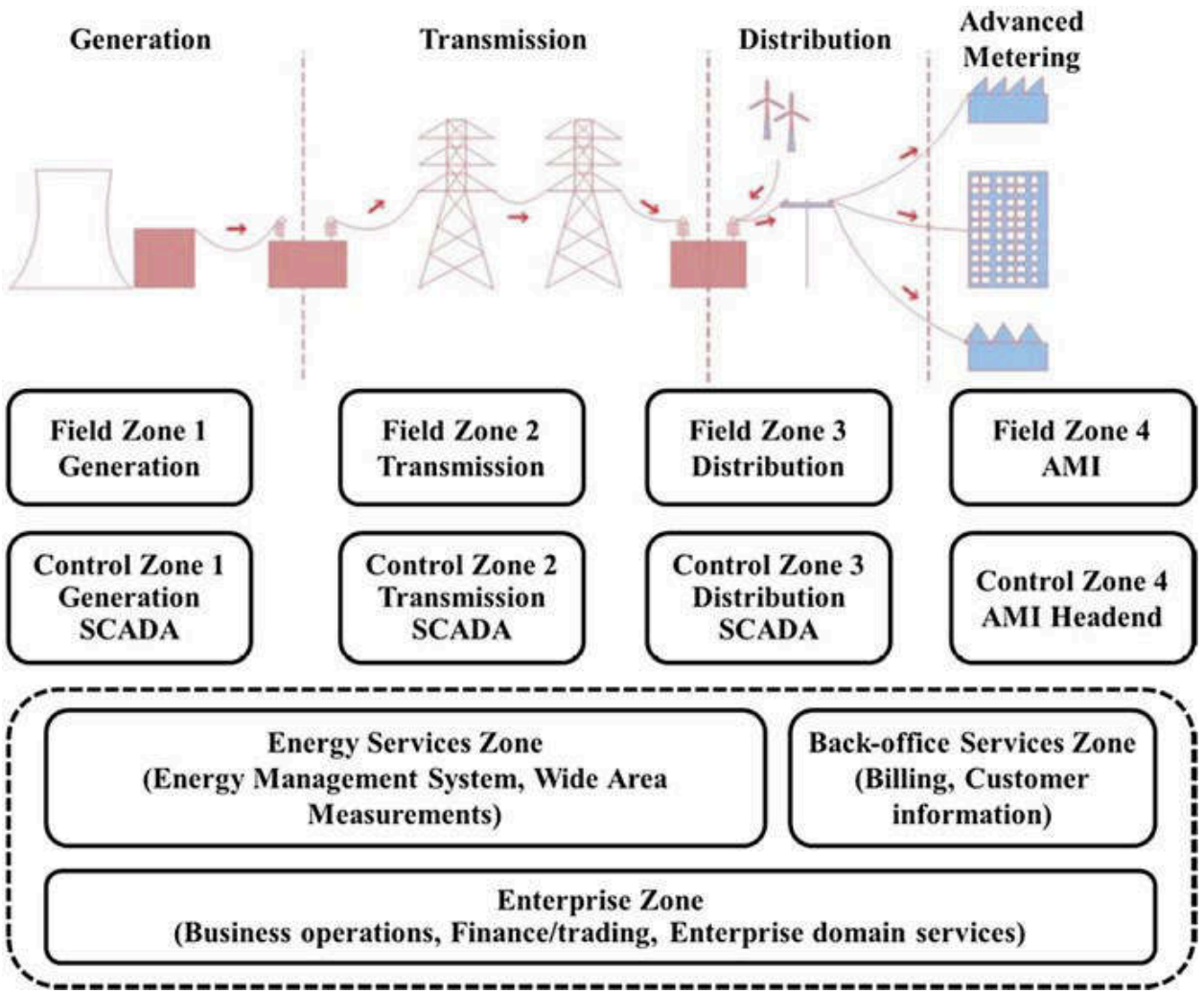
Security of field zone components

- As discussed before, security of field zone components is often limited to physical security
- ‘Normal’ IT security mechanisms do not apply
  - Firewalls or IDS/IPS for control networks?
  - Anti-virus for PLCs/embedded systems?
  - Often the legacy systems, components and networks are present
- Is field zone more susceptible to attack or enterprise zone? Why?
- The enemy who attacks the CPS will try use the enterprise and control zones to disturb the field zone
- Such an attacker must not be taken lightly!

CPS Application: Smart Power Grid



CPS Application: Smart Power Grid



Cyber-security of SCADA and Other Industrial Control Systems by Colbert & Kott

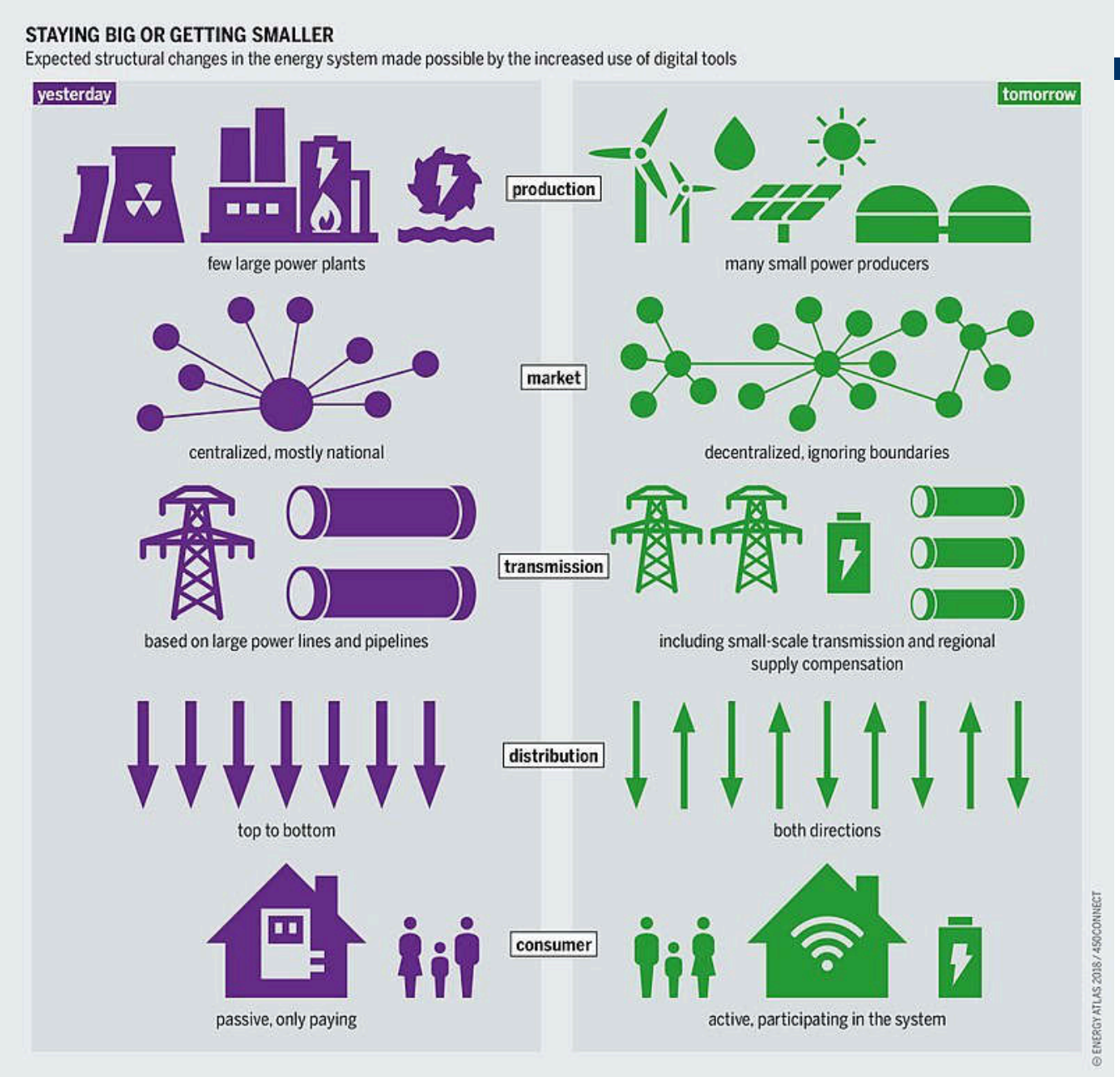


Image by Bartz/Stockmar, CC BY-SA 4.0, https://commons.wikimedia.org/w/index.php?curid=69505750

US Policy on Smart Grid

It is the policy of the United States to support the modernization of the Nation's electricity transmission and distribution system to maintain a reliable and secure electricity infrastructure that can meet future demand growth and to achieve each of the following, which together characterize a Smart Grid:

(1) Increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid.

(2) Dynamic optimization of grid operations and resources, with full cyber-security.

(3) Deployment and integration of distributed resources and generation, including renewable resources.

(4) Development and incorporation of demand response, demand-side resources, and energy-efficiency resources.

(5) Deployment of 'smart' technologies (real-time, automated, interactive technologies that optimize the physical operation of appliances and consumer devices) for metering, communications concerning grid operations and status, and distribution automation.

(6) Integration of 'smart' appliances and consumer devices.

(7) Deployment and integration of advanced electricity storage and peak-shaving technologies, including plug-in electric and hybrid electric vehicles, and thermal storage air conditioning.

(8) Provision to consumers of timely information and control options.

(9) Development of standards for communication and interoperability of appliances and equipment connected to the electric grid, including the infrastructure serving the grid.

EU Vision of Smart Grid

- The European Union Commission Task Force for Smart Grids provides smart grid definition[10] as:
- "A Smart Grid is an electricity network that can cost efficiently integrate the behaviour and actions of all users connected to it – generators, consumers and those that do both – in order to ensure economically efficient, sustainable power system with low losses and high levels of quality and security of supply and safety. A smart grid employs innovative products and services together with intelligent monitoring, control, communication, and self-healing technologies in order to:
  - Better facilitate the connection and operation of generators of all sizes and technologies.
  - Allow consumers to play a part in optimising the operation of the system.
  - Provide consumers with greater information and options for how they use their supply.
  - Significantly reduce the environmental impact of the whole electricity supply system.
  - Maintain or even improve the existing high levels of system reliability, quality and security of supply.
  - Maintain and improve the existing services efficiently."

A common element to most definitions is the application of digital processing and communications to the power grid, making data flow and information management central to the smart grid.

Thanks a lot

If you are taking a Nap, **wake up**.....Lecture Over